

Application No. 09/950,432
Amendment dated October 7, 2004
Reply to Office Action of July 7, 2004

1 Amendments to the Claims:

2 This listing of claims will replace all prior versions and listings of claims in the application:
3

4 Listing of Claims:

5 1. (currently amended) A method of authenticating a host to receive content from a storage
6 engine, device, the method comprising:
7 receiving at the storage engine a certificate from the host device, the certificate
8 including a plurality of fields, including a field holding a digital signature
9 from a certifying authority;
10 verifying the digital signatures in the certificate, the verifying including at least one
11 of:
12 verifying the certifying authority digital signature using the certifying
13 authority public key; and
14 verifying a device host digital signature using a host device public key ; and
15 receiving validation data from a source, the validation data identifying one or more
16 data in the certificate as valid or invalid according to predetermined criteria;
17 and
18 if the digital signatures are verified and validated, generating a random number at the
19 storage engine and encrypting the random number with a public key extracted
20 from the certificate to form a session key and transmitting a the session key to
21 the device host;
22 at the host, receiving an encrypted content key from the storage engine; and
23 decrypting the encrypted content key using the session key to recover the content key
24 to establish a secure communication channel.

1 2. (original) The method of claim 1 wherein the source is one of a portable medium and
2 firmware.

1 3. (cancelled)

1 4. (cancelled)

Application No. 09/950,432
Amendment dated October 7, 2004
Reply to Office Action of July 7, 2004

1 5. (currently amended) The method of claim 1 wherein the certifying of the host device
2 includes certifying a second host for a host to second host secure communication channel, ~~the~~
3 certifying allowing a copy function between the host and the second host.

1 6. (currently amended) The method of claim 1 wherein the data in the certificate specifies ~~one~~
2 or more of a product category, a product line, a model, a revision and a serial number of ~~the~~
3 ~~device~~ host.

1 7. (currently amended) The method of claim 6 wherein the source validation data is compared
2 with the data in the certificate to identify as invalid one or more of the product category, ~~the~~
3 product line, the model, the revision and the serial number of the ~~device~~ host.

1 8. (currently amended) The method of claim 1 wherein the certificate includes one or more of
2 a certifying authority identifier field, a version field, a sign key identifier field, an exposed
3 methods field, a company field, a model identifier field, a revision field, a metadata identifier
4 field, a device digital signature key field, a certifying authority digital signature field, a serial
5 number field, a protocol public key field and a device digital signature field, wherein the
6 certifying authority digital signature verifies one or more of the fields in the certificate and
7 the ~~device~~ host digital signature verifies one or more of the fields in the certificate.

1 9. (currently amended) The method of claim 1 wherein the certificate enables an entity
2 receiving the certificate to control the quality of the ~~device~~ host by invalidating ~~devices~~ hosts
3 that are false or have latent defects.

1 10. (currently amended) The method of claim 6 wherein the certificate further includes fields
2 provided by a ~~device~~ host manufacturer, including the company public key, wherein the
3 company public key is digitally signed by the certifying authority.

1 11. (currently amended) The method of claim 6 wherein the certificate further includes fields
2 provided by a ~~device~~ host manufacturer, the fields including the ~~device~~ host public key,
3 wherein the ~~device~~ host public key is digitally signed by the company.

Application No. 09/950,432
Amendment dated October 7, 2004
Reply to Office Action of July 7, 2004

1 12. (currently amended) The method of claim 6 wherein one or more of the product category, ---
2 the product line, the model, the revision and the serial number of the ~~device~~ host are provided
3 to a certificate creator after the ~~device~~ host passes a qualification procedure.

1 13. (original) The method of claim 1 wherein the certificate specifies one or more certificate
2 classes, the certificate classes providing a set of methods that may be exposed after the
3 transmitting the session key.

1 14. (currently amended) The method of claim 13 wherein the set of methods includes digital
2 rights management (DRM) methods include one or more of a copy method, a record method,
3 a play method, a read secure metadata method, a write secure metadata method, and an
4 unlock method, the DRM methods operable according to a type of the ~~device~~ host.
5

1 15. (cancelled)

1 16. (original) The method of claim 1 wherein each of the fields hold 326-bit values for 163-
2 bit elliptic curve cryptography.

1 17. (original) The method of claim 1 wherein the certifying authority public key is referenced
2 by a field of the certificate.

1 18. (currently amended) The method of claim 1 wherein the certifying authority public key is
2 in a the firmware component.
3

1 19. (cancelled)

1 20. (currently amended) ~~An~~ A storage engine configured to certify a host, the engine
2 comprising:
3 a firmware component including:
4 a block configured to receive a certificate from the host, the certificate
5 including a plurality of fields, including a field holding a protocol public key;

Application No. 09/950,432
Amendment dated October 7, 2004
Reply to Office Action of July 7, 2004

6 a block configured to verify one or more digital signatures in the certificate,
7 including at least one of:
8 a certifying authority digital signature using a certifying authority
9 public key; and
10 a device digital signature using a device public key in the certificate;
11 and
12 a block configured to receive validation data from a source, the validation data
13 identifying one or more data in the certificate as valid or invalid according to
14 predetermined criteria; and
15 a block configured to transmit a session key to the host ~~to establish a secure~~
16 ~~communication channel~~ when the digital signatures are verified and validated; and
17 a block to transmit an encrypted content key to the host, wherein the host is
18 enabled to recover a content key from the encrypted content key by using the session
19 key.

20
21
22 Claims 21-23. (cancelled)